身份认证体系在新媒体中的研究与实践

摘　要：新媒体作为互联网时代信息化技术的产物，其开放性、互动性、及时性、移动性等特点在一定程度上给人们带来了方便快捷的享受，但随之带来的信息安全问题也是层出不穷的，尤其是在新媒体环境下，普通用户也可以通过各种方式参与到新闻信息的生产加工之中，因此，对如何运用多因素身份认证体系确保新闻信息采集传输过程中的保密性、完整性以及可用性，包括新闻信息发布者、接收者的身份真实性以及信息传输通道的安全性等问题的深入研究具有非常重要的意义。

关键词：新媒体；信息安全；多因素身份认证；认证体系
中图分类号：G202　　文献标识码：A
文章编号：1671-0134（2017）04-108-02　　DOI：10.19483/j.cnki.11-4653/n.2017.04.033

■文 / 胡鹏程

引言

随着科学技术的进步、互联网的加速发展，微传播时代的到来对传统媒体的发展和转型起到了深远的影响，网络的发展带来了新媒体业务的繁荣，互联网的信息资源已远远超过了广播、电视、报纸等传统媒体[1]。网络新媒体由于其具有开放性、互动性、及时性、移动性等特点在一定程度上给人们带来方便快捷的享受，但一部分“网络政治动员”冒用合法媒体人的身份，借助网络的方式发布误导、煽动或者是其他目的的信息，这些信息安全问题都给新媒体的发展带来了巨大的挑战。媒体人作为新媒体的传播者、引导者、服务者以及监督者，在更加迅速准确地报道新闻、引导舆论、服务社会的同时，应该斩断政治动员虚拟转换的关键节点，有效避其对网民进行鼓动、诱惑乃至操纵，从而引发政治权利的改变，削弱国家权威，影响国家政治安定和社会稳定等安全问题。

1. 背景简介

21 世纪以来，在市场扩张与技术演进的双轮驱动之下，互联网与新媒体进入高速发展阶段。新媒体广泛地融入我国政治、经济、社会和文化等多个领域，已成为受众获取讯息、分享娱乐和表达诉求的主要媒介[2]。新媒体彻底改变了传统媒体时代专业采编、单向传播、单次传播的模式，受众参与、采编互动、融合传播、场景切入、跨平台联动成为新特征，其强大的全球政治宣传和政治动员的力量，使之成为影响国家政治安全的关键因素。

网络和新媒体时代的信息安全问题随着信息技术的飞跃发展和广泛应用而凸显，并渗透到新闻信息采集传输发布的各个阶段，因此我们要从以下三个方面考虑新媒体环境下新闻信息采集传输的安全性：首先是要保证信息不能以任何方式泄露，其次要保证信息的完整性以及真实性，再次就是要防止信息在没有被授权和允许的情况下被复制，并且其所依附的系统必须要具备高度的安全和可靠。身份认证是信息安全体系的重要组成部分，经历了从软件到硬件认证，从单认证因素到多因素认证，从静态认证到动态认证的过程，并且随着生物识别技术的发展，基于生物特征的用户身份认证技术受到人们的青睐，包括指纹、虹膜、语音、面部提取生物特征等。身份认证技术正朝着更加安全、易用，多种技术手段相结合的方向发展，以建立安全、高效、简洁的认证系统。

2. 身份认证技术简介

2.1 传统身份认证技术简介

传统身份认证采用的识别机制是“用户账户 + 静态口令”[3-4]，因为不法分子容易盗取用户的用户名，实际上传统身份认证只是单因素认证，静态口令是确保其安全性的依据。传统认证方式具有简单性、操作性等特点，但是缺乏安全性。

2.2 多因素认证常用技术

2.2.1 令牌认证技术

随着网络技术的发展，为了更好地保护使用者的帐号、密码安全，推出了动态口令认证技术，也称作令牌认证技术[5-7]，即每隔 60 秒钟，自动依照特别的算法生成一组新的随机密码，该随机密码又称为动态口令，或一次性密码。其包括基于时间的同步密码技术、基于事件的同步密码技术以及挑战 · 应答异步密码技术三种。

2.2.2 生物识别技术

生物识别技术是目前最为方便和安全的识别技术，不容易被冒充模拟或窃取，并解决了传统的钥匙等物品易遗忘的问题，使用起来既方便又不需要定期维护，比传统身份认证方式更方便、更安全。已经用于身份识别的人体生理特征有脸像、指纹、虹膜、DNA 等[8-10]；行为特征有步态、签名等。生物识别技术的应用在过去 2 年内增长显著，借助生物识别技术，可以有效保证被识别生物的各种信息是安全可靠的，同时还要保障应用以及系统之间互动不变。

3. 身份认证体系在新媒体环境下的实践

新媒体环境下新闻信息是利用数字技术，通过互联网、无线通信网络等渠道，以手机或者计算机为采集或接收终端，进行即时互动信息交流和传播。为保证新闻信息采集传输的安全性，本文采用基于 PKI/CA 多因素认证体系为合法用户颁发数字证书，并且通过灵活多样的认证方式满足不同类型

的终端用户，有效降低单个因子所存在的安全风险，提供认证的安全性，通过单点登录实现一次登录，安全同行；并充分考虑复杂网络环境下的数据传输安全性，针对传输过程中可能面临的信息截取、内容泄露或者内容篡改等安全风险，有针对性地采取数据安全防护手段。

本文基于新华社新闻信息采集平台提出的多因素认证体系，从架构上包含密码基础设施、安全支撑平台、上层应用等，是一个整体性的安全服务平台，并通过一套监控审计系统实时有效监测平台的安全服务能力以及对上层应用的安全保障能力，将运行状态通过报表、图标等形式绘出后进行详细展示。

3.1 总体框架

本文基于 PKI 技术的安全总体框架如下图所示：

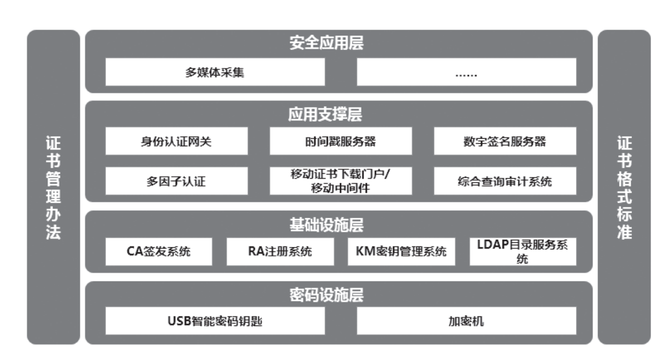


图 1 总体框架图

用户身份鉴别。由 CA 签发系统、RA 注册系统、KM 密钥管理系统、加密机和 LDAP 目录服务系统组成，作为 PKI/CA 证书认证体系的基础设施，负责发放和管理数字证书，并将用户证书和黑名单信息发布到 LDAP 目录服务中，USB 智能密码钥匙可为数字证书存储介质，通过数字证书方式进行用户身份标识，加密机分别为 CA 签发系统和 RA 注册系统提供密钥的安全存储和高速的密码运算服务。

统一身份认证。通过多因子认证平台为新闻信息采集平台提供多种认证方式，用户可以根据不同的终端登陆方式选择不同的认证方法，例如指纹识别、动态口令等，通过与身份认证网关联动为平台用户提供基于数字证书的高强度身份认证。移动证书下载门户可以实现移动证书的下载服务，通过移动中间件可以为移动端实现证书认证。

数字签名服务。数字签名服务器采用数字签名技术，配合时间戳技术可以实现稿件在某一时间节点传递过程中内容保密、完整以及操作的不可抵赖等功能。

数字证书综合统计查询系统。提供证书发放情况和使用情况的统一展现平台，实现数字证书数据、基于数字证书的行为审计数据。

同时，为了证书发放的规范运营，明确证书管理员的工作职责，还制定了一系列的证书管理办法。为了满足证书的安全应用，制定本行业、本企业的证书格式规范，确保证书信息能方便被应用系统识别和调用。

3.2 逻辑架构

本文充分考虑新闻信息采集业务现状以及身份标识统一管理、统一身份认证、数据传输安全等安全需求，并对业务使用场景进行深入分析，基于 PKI 技术的新闻信息采集平台安全设计的逻辑架构如下图所示：

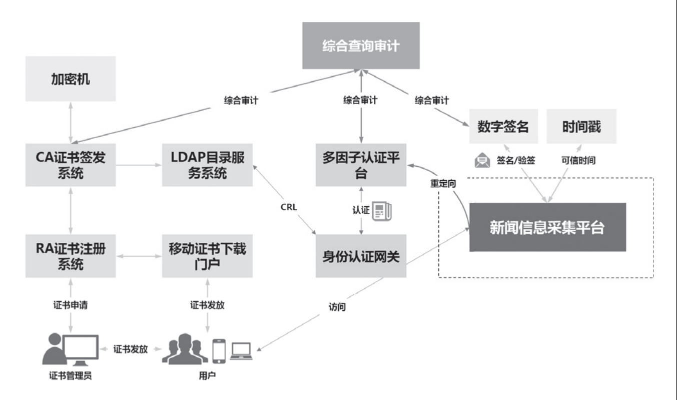


图 2 逻辑架构图

4. 小结与展望

新媒体革命对身份认证是机遇也是挑战。新闻信息从产生、传输、存储到利用的每一个环节都存在信息泄露的隐患，因此，利用多因素身份认证技术对这一过程中增加强有力的加密是最常规也是最有效的安全防护措施，并且借助生物识别技术，可以有效保证被识别生物的信息是安全可靠的，从根源上对新闻信息进行有效的管控，在虚拟空间内树立国家权威。媒

参考文献

[1] 洪杰文，归伟夏. 新媒体技术 [M]. 重庆：西南师范大学出版社，2016.

[2] 杨西京 . 如何推进传统出版与新媒体融合发展 [J]. 科技与出版，2014（11）：8-10.

[3] 林元明 . 基于手机令牌的身份认证系统的研究与实现 [D]. 厦门：厦门大学，2009.

[4] 范良云 . 基于 121 令、手机令牌与生物特征的身份认证系统研究与实现 [D]. 厦门：厦门大学，2010.

[5]lfredJ.Menezes，PaulC.vanOorschot，ScottA.Vanstone.HandbookofAppliedCryptography[M].

[6] 季晓玉 . 动态口令双向身份认证系统的研究与实现 [D]. 大连：大连理工大学，2008.

[7] 王蕴红，谭铁牛 . 现代身份鉴别新技术：生物特征识别技术 [J]. 中国基础科学，2000，9（1）：4-10.

[8]BolleRM，ConnellJ，PankantiS，eta1.Biometrics101[R].ReportRC22481.mMResearch，2002.

[9]MaltoniD，MaioD，JainAl（’eta1.HandbookofHngerprintRecognition[C].NewYork：Springer-Veflag，Inc.，2003.

[10] 蔡皖东 . 网络与信息安全 [M]. 北京：西北工业大学出版社，2004.

（作者单位：新华通讯社通信技术局）